

Approximating the Closest Vector Problem Using an Approximate Shortest Vector Oracle

Chandan Dubey* and Thomas Holenstein

Institute for Theoretical Computer Science
ETH Zurich
chandan.dubey@inf.ethz.ch
thomas.holenstein@inf.ethz.ch

Abstract. We give a polynomial time Turing reduction from the $\gamma^2\sqrt{n}$ -approximate closest vector problem on a lattice of dimension n to a γ -approximate oracle for the shortest vector problem. This is an improvement over a reduction by Kannan, which achieved $\gamma^2n^{\frac{3}{2}}$.

1 Introduction

A *lattice* is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ in \mathbb{R}^m . These vectors are also referred to as a *basis* of the lattice. The *successive minima* $\lambda_i(\mathbb{L})$ (where $i = 1, \dots, n$) for the lattice \mathbb{L} are among the most fundamental parameters associated to a lattice. The value $\lambda_i(\mathbb{L})$ is defined as the smallest r such that a sphere of radius r centered around the origin contains at least i linearly independent lattice vectors. Lattices have been investigated by computer scientists for a few decades after the discovery of the LLL algorithm [14]. More recently, Ajtai [1] showed that lattice problems have a very desirable property for cryptography: they exhibit a worst-case to average-case reduction.

We now describe some of the most fundamental and widely studied lattice problems. Given a lattice \mathbb{L} , the γ -approximate shortest vector problem (γ -SVP for short) is the problem of finding a non-zero lattice vector of length at most $\gamma\lambda_1(\mathbb{L})$. Let the minimum distance of a point $\mathbf{t} \in \mathbb{R}^m$ from the lattice \mathbb{L} be denoted by $\mathbf{d}(\mathbf{t}, \mathbb{L})$. Given a lattice \mathbb{L} and a point $\mathbf{t} \in \mathbb{R}^m$, the γ -approximate closest vector problem or γ -CVP for short is the problem of finding a $\mathbf{v} \in \mathbb{L}$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \gamma\mathbf{d}(\mathbf{t}, \mathbb{L})$.

Besides the search version just described, CVP and SVP also have a gap version. The problem $\text{GapCVP}_\gamma(\mathbf{B}, \mathbf{t})$ asks the distance of \mathbf{t} from the lattice $\mathbb{L}(\mathbf{B})$ within a factor of γ , and $\text{GapSVP}_\gamma(\mathbf{B})$ asks for $\lambda_1(\mathbf{B})$ within a factor of γ . This paper deals with the search version described above.

The problems CVP and SVP are quite well studied. The Gap versions of the problems are arguably easier than their **search** counterparts. We know that CVP

* Chandan Dubey is partially supported by the Swiss National Science Foundation (SNF), project no. 200021-132508

and **SVP** can be solved exactly in deterministic $2^{O(n)}$ time [18, 4]. In polynomial time they can be approximated within a factor of $2^{n(\log \log n)/\log n}$ using LLL [14] and subsequent improvements by Schnorr [21] and Micciancio et. al. [18] (for details, see the book by Micciancio and Goldwasser [9]). On the other hand, it is known that there exists $c > 0$, such that no polynomial time algorithm can approximate **GapCVP** and **GapSVP** within a factor of $n^{c/\log \log n}$, unless $\mathbf{P} = \mathbf{NP}$ or another unlikely scenario is true [7, 10]. The security of hardness of cryptosystems following Ajtai's seminal work [1] is based on the worst-case hardness of $\tilde{O}(n^2)$ -**GapSVP** [20, 19, 15]. In the hardness area, **CVP** is much more understood than **SVP**. For example, as opposed to **CVP**, until now all known **NP**-hardness proofs for **SVP** [2, 17, 13, 10] are randomized. A way to prove deterministic hardness of **SVP** is to prove better reductions from **CVP** to **SVP**. This paper aims to study and improve the known relations between these two problems.

A very related result is from Kannan [11], who gave a way to solve \sqrt{n} -**CVP** using an exact **SVP** oracle. A generalization of his reduction was used to solve **CVP** within a factor of $(1 + \epsilon)$ by reducing it to sampling short vectors in the lattice [3]. The improvement from \sqrt{n} to $(1 + \epsilon)$ is achieved mainly because the reduction uses $2^{O(n)}$ time instead of polynomial. It is also known that a γ -**CVP** oracle can be used to solve γ -**SVP** [8].

In a survey [12], Kannan gave a different reduction from $\gamma^2 n^{\frac{3}{2}}$ -**CVP** to γ -**SVP**. A few words of comparison between our methods and the method used by Kannan [12]. Kannan uses the dual lattice (denoted by $\mathbf{B}^* = (\mathbf{B}^T)^{-1}$, where \mathbf{B}^T is the transpose of the matrix \mathbf{B}) and the transference bound $\lambda_1(\mathbf{B})\lambda_1(\mathbf{B}^*) \leq n$ to find a candidate close vector. Due to the fact that he applies the **SVP** oracle on both \mathbb{L} as well as \mathbb{L}^* , he loses an additional factor of n . Our method does not use the dual lattice.

Our contribution: We improve the result by Kannan [12], which shows that $\gamma^2 n^{3/2}$ -**CVP** can be solved using an oracle to solve γ -**SVP**, and solve $\gamma^2 \sqrt{n}$ -**CVP** using the same oracle.

For this, we essentially combine the earlier result by Kannan [11] with a reduction by Lyubashevsky and Micciancio [15], as we explain now in some detail.

Our starting point is the earlier reduction by Kannan, which solves \sqrt{n} -**CVP** using an exact **SVP**-oracle. In order to explain our ideas, we first shortly describe his reduction. Given a **CVP**-instance $\mathbf{B} \in \mathbb{Q}^{m \times n}$, $\mathbf{t} \in \mathbb{R}^m$, Kannan uses the **SVP**-oracle to find $\lambda_1(\mathbf{B})$. He then creates the new basis $\tilde{\mathbf{B}} = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ 0 & \alpha \end{bmatrix}$, where he picks α carefully somewhat smaller than $\lambda_1(\mathbf{B})$. Now, if $\mathbf{d}(\mathbf{t}, \mathbf{B})$ is significantly smaller than $\lambda_1(\mathbf{B})$ (say, $\lambda_1(\mathbf{B})/3$), then the shortest vector in $\tilde{\mathbf{B}}$ is $\begin{bmatrix} \mathbf{t}^\dagger - \mathbf{t} \\ -\alpha \end{bmatrix}$, where \mathbf{t}^\dagger is the lattice vector closest to \mathbf{t} (i.e., the vector we are trying to find). On the other hand if $\mathbf{d}(\mathbf{t}, \mathbf{B})$ is larger than $\lambda_1(\mathbf{B})/3$, then Kannan projects the instance in the direction orthogonal to the shortest vector of $\tilde{\mathbf{B}}$. This reduces the dimension by 1, and an approximation in the resulting instance can be used to get an

approximation in the original instance, because the projected approximation can be “lifted” to find some original lattice point which is not too far from \mathbf{t} .

We show that in case we only have an approximation oracle for SVP, we can argue as follows. First, if $d(\mathbf{t}, \mathbf{B}) \leq \frac{\lambda_1(\mathbf{B})}{2\gamma}$, then we have an instance of a so called “Bounded Distance Decoding” problem. By a result of Lyubashevsky and Micciancio [15], this can be solved using the oracle we assume. In case $d(\mathbf{t}, \mathbf{B}) > \frac{\lambda_1(\mathbf{B})}{2\gamma}$ we can recurse in the same way as Kannan does. The approximation factor $\gamma^2 \sqrt{n}$ comes from this case: lifting a projection after the recursion returns, incurs an error of roughly the half the length of the vector \mathbf{v} which was used to project. Since this \mathbf{v} can have length almost $\gamma \lambda_1(\mathbf{B})$, the length of \mathbf{v} can be almost a factor γ^2 larger than $d(\mathbf{t}, \mathbf{B})$. The squares of these errors then add up as in Kannan’s reduction, which gives a total approximation factor of $\gamma^2 \sqrt{n}$.

We remark that even though we do not know which of the two cases apply, we can simply run both, and then use the better result.

Finally, we would like to mention that to the best of our knowledge there is no published proof that in Kannan’s algorithm [11] the projected bases have a representation which is polynomial in the input size. We show that this is indeed the case. For this, it is essentially enough to use a lemma from [9] which states that the vectors in a Gram-Schmidt orthogonalization have this property.

2 Preliminaries

2.1 Notation

A lattice basis is a set of linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$. It is sometimes convenient to think of the basis as an $n \times m$ matrix \mathbf{B} , whose n columns are the vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$. The lattice generated by the basis \mathbf{B} will be written as $\mathbb{L}(\mathbf{B})$ and is defined as $\mathbb{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} | \mathbf{x} \in \mathbb{Z}^n\}$. The *span* of a basis \mathbf{B} , denoted as $\text{span}(\mathbf{B})$, is defined as $\{\mathbf{B}\mathbf{y} | \mathbf{y} \in \mathbb{R}^n\}$. We will assume that the lattice is over rationals, i.e., $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{Q}^m$, and the entries are represented by the pair of numerator and denominator. An *elementary* vector $v \in \mathbb{L}(\mathbf{B})$ is a vector which cannot be written as a non-trivial multiple of another lattice vector.

A *shortest vector* of a lattice is a non-zero vector in the lattice whose ℓ_2 norm is minimal. The length of the shortest vector is $\lambda_1(\mathbf{B})$, where λ_1 is as defined in the introduction. For a vector $\mathbf{t} \in \mathbb{R}^m$, let $d(\mathbf{t}, \mathbb{L}(\mathbf{B}))$ denote the distance of \mathbf{t} to the closest lattice point in \mathbf{B} . We use \mathbf{t}^\dagger to denote a (fixed) closest vector to \mathbf{t} in $\mathbb{L}(\mathbf{B})$.

For two vectors \mathbf{u} and \mathbf{v} in \mathbb{R}^m , $\mathbf{v}|_{\mathbf{u}}$ denotes the component of \mathbf{v} in the direction of \mathbf{u} i.e., $\mathbf{v}|_{\mathbf{u}} = \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} \mathbf{u}$. Also, the component of \mathbf{v} in the direction orthogonal to \mathbf{u} is denoted by $\mathbf{v}_{\perp \mathbf{u}}$ i.e., the vector $\mathbf{v} - \mathbf{v}|_{\mathbf{u}}$.

Consider a lattice $\mathbb{L}(\mathbf{B})$ and a vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ in the lattice. Then the projected lattice of $\mathbb{L}(\mathbf{B})$ perpendicular to \mathbf{v} is $\mathbb{L}(\mathbf{B}_{\perp \mathbf{v}}) := \{\mathbf{u}_{\perp \mathbf{v}} | \mathbf{u} \in \mathbb{L}(\mathbf{B})\}$. A basis of $\mathbb{L}(\mathbf{B}_{\perp \mathbf{b}_1})$ is given by the vectors $\{\mathbf{b}_{2 \perp \mathbf{b}_1}, \dots, \mathbf{b}_{n \perp \mathbf{b}_1}\}$.

For an integer $k \in \mathbb{Z}^+$ we use $[k]$ to denote the set $\{1, \dots, k\}$.

2.2 Lattice Problems

In this paper we are concerned with the following approximation problems, which are parametrized by some $\gamma > 1$.

γ -SVP: Given a lattice basis \mathbf{B} , find a non-zero vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v}\| \leq \gamma \lambda_1(\mathbf{B})$.

γ -CVP: Given a lattice basis \mathbf{B} , and a vector $\mathbf{t} \in \mathbb{R}^m$ find a vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \gamma d(\mathbf{t}, \mathbf{B})$.

We also use the following promise problems, which are parameterized by some $\gamma > 0$.

γ -BDD: Given a lattice basis \mathbf{B} , and a vector $\mathbf{t} \in \mathbb{R}^m$ with the promise that $d(\mathbf{t}, \mathbb{L}(\mathbf{B})) \leq \gamma \lambda_1(\mathbf{B})$, find a vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v} - \mathbf{t}\| = d(\mathbf{t}, \mathbf{B})$.

γ -uSVP: Given a lattice basis \mathbf{B} with the promise that $\lambda_2(\mathbf{B}) \geq \gamma \lambda_1(\mathbf{B})$, find a non-zero vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v}\| = \lambda_1(\mathbf{B})$ (this makes sense only for $\gamma \geq 1$).

We assume that we have given a γ -SVP oracle, denoted by \mathfrak{D} . When given a set of linearly independent vectors $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\} \in \mathbb{Q}^{m \times n}$, $\mathfrak{D}(\mathbf{B})$ returns an elementary vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ which satisfies $0 < \|\mathbf{v}\| \leq \gamma \lambda_1(\mathbb{L}(\mathbf{B}))$ (if \mathbf{v} is not elementary then we can find out the multiple and recover the corresponding elementary vector).

3 Some basic tools

Given a basis \mathbf{B} and an elementary vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$, we can in polynomial time find a new basis of $\mathbb{L}(\mathbf{B})$ of the form $\{\mathbf{v}, \mathbf{b}_2', \dots, \mathbf{b}_n'\}$. To do this we use the following lemma from Micciancio [16] (page 7, Lemma 1), which we specialized somewhat for our needs.

Lemma 1. *There is a polynomial time algorithm $\text{findbasis}(\mathbf{v}, \mathbf{B})$, which, on input an elementary vector \mathbf{v} of $\mathbb{L}(\mathbf{B})$ and a lattice basis $\mathbf{B} \in \mathbb{Q}^{m \times n}$ outputs $\tilde{\mathbf{B}} = (\tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_n)$ such that $\mathbb{L}(\mathbf{v}, \tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_n) = \mathbb{L}(\mathbf{B})$.*

Lemma 2. *Let $\mathbb{L}(\mathbf{B})$ be a lattice and $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ be a vector in the lattice. If $\mathbb{L}(\mathbf{B}_{\perp \mathbf{v}})$ is the projected lattice of $\mathbb{L}(\mathbf{B})$ perpendicular to \mathbf{v} then $\lambda_i(\mathbf{B}_{\perp \mathbf{v}}) \leq \lambda_{i+1}(\mathbf{B})$, $i \in [n-1]$.*

Proof. Let \mathbf{v}_i be the vector of length $\lambda_i(\mathbf{B})$ such that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ are linearly independent. A set of such vectors exists [9]. If $(\mathbf{v}_1)_{\perp \mathbf{v}} = 0$ then $(\mathbf{v}_{i>1})_{\perp \mathbf{v}} \in \mathbb{L}(\mathbf{B}_{\perp \mathbf{v}})$ and $0 < \|(\mathbf{v}_i)_{\perp \mathbf{v}}\| \leq \|\mathbf{v}_i\|$, proving the lemma. If $(\mathbf{v}_1)_{\perp \mathbf{v}} \neq 0$ then $(\mathbf{v}_1)_{\perp \mathbf{v}} \in \mathbb{L}(\mathbf{B}_{\perp \mathbf{v}})$ and $0 < \|(\mathbf{v}_1)_{\perp \mathbf{v}}\| \leq \|\mathbf{v}_1\|$. We argue in a similar way with $(\mathbf{v}_2)_{\perp \mathbf{v}}$ to prove the lemma for $i > 1$. \square

We use the following reduction from due to Lyubashevsky and Micciancio [15].

Theorem 1. *For any $\gamma \geq 1$, there is a polynomial time oracle reduction from $\text{BDD}_{\frac{1}{2\gamma}}$ to uSVP_{γ} .*

For completeness, we sketch a proof of Theorem 1 in Appendix A.

4 Reducing CVP to SVP

We prove the following theorem:

Theorem 2. *Given a basis $\mathbf{B} \in \mathbb{Q}^{m \times n}$ and a vector $\mathbf{t} \in \mathbb{R}^m$, the problem $\gamma^2 \sqrt{n}$ -CVP is Turing reducible to the problem γ -SVP in time $\text{poly}(n, \log \gamma, \max_i \log \|\mathbf{b}_i\|)$.*

In this section we give the algorithm to prove our theorem, and show that once it terminates, it satisfies the requirements of the theorem. We will show that the algorithm runs in polynomial time in the next section.

The reduction takes as an input a basis $\mathbf{B} \in \mathbb{Q}^{m \times n}$ and a vector $\mathbf{t} \in \mathbb{R}^m$. Recall that the oracle \mathfrak{O} takes as input a basis over \mathbb{Q} and outputs an elementary vector which is a γ -approximation to the shortest vector. The reduction is given in Algorithm 1.

Algorithm 1 CVP(\mathbf{B}, \mathbf{t}) (input: $\mathbf{B} \in \mathbb{Q}^{m \times n}, \mathbf{t} \in \mathbb{Q}^m$)

```

1: if  $n = 1$  then
2:   Let  $\mathbf{b}_1$  be the only column of  $\mathbf{B}$ .
3:   return  $a\mathbf{b}_1$  with  $a \in \mathbb{Z}$  such that  $\|a\mathbf{b}_1 - \mathbf{t}\|$  is minimal.
4: else
5:    $\mathbf{z}_1 \leftarrow \frac{1}{2\gamma}$ -BDD( $\mathbf{B}, \mathbf{t}$ ) (Solve this with calls to  $\mathfrak{O}$  as in Theorem 1 )
6:    $\mathbf{v} \leftarrow \mathfrak{O}(\mathbf{B})$ 
7:    $\{\mathbf{b}_2, \dots, \mathbf{b}_n\} \leftarrow \text{LLL}(\text{findbasis}(\mathbf{v}, \mathbf{B}))$ 
8:    $\forall i \in \{2, \dots, n\} : (\mathbf{b}'_i)_{\perp \mathbf{v}} \leftarrow \mathbf{b}_i - \mathbf{b}_i|_{\mathbf{v}}$ 
9:    $\mathbf{B}'_{\perp \mathbf{v}} \leftarrow \{(\mathbf{b}'_2)_{\perp \mathbf{v}}, \dots, (\mathbf{b}'_n)_{\perp \mathbf{v}}\}$ 
10:   $\mathbf{t}'_{\perp \mathbf{v}} \leftarrow \mathbf{t} - \mathbf{t}|_{\mathbf{v}}$ 
11:   $\mathbf{z}'_2 \leftarrow \text{CVP}(\mathbf{B}'_{\perp \mathbf{v}}, \mathbf{t}'_{\perp \mathbf{v}})$ 
12:  Find  $(a_2, \dots, a_n) \in \mathbb{Z}^{n-1}$  such that  $\mathbf{z}'_2 = \sum_{i=2}^n a_i (\mathbf{b}'_i)_{\perp \mathbf{v}}$ 
13:  Find  $a_1 \in \mathbb{Z}$  such that  $\mathbf{z}_2 = a_1 \mathbf{v} + \sum_{i=2}^n a_i \mathbf{b}_i$  is closest to  $\mathbf{t}$ 
14:  return the element of  $\{\mathbf{z}_1, \mathbf{z}_2\}$  which is closest to  $\mathbf{t}$ .
15: end if

```

In line 6, we can simulate an oracle for $\frac{1}{2\gamma}$ -BDD due to Theorem 1, given \mathfrak{O} . In line 7 we run the LLL algorithm on the basis returned by `findbasis`; this is an easy way to ensure that the representation of the basis does not grow too large (cf. the proof of Lemma 5). The optimization problem in line 13 is of course easy to solve: for example, we can find $a'_1 \in \mathbb{R}$ which minimizes the expression and then round a'_1 to the nearest integer.

Theorem 3. *The approximate CVP-solver (Algorithm 1) outputs a vector $\mathbf{z} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{z} - \mathbf{t}\| \leq \gamma^2 \sqrt{n} d(\mathbf{t}, \mathbf{B})$.*

Proof. We prove the theorem by induction on n . For the base case (i.e., $n = 1$) we find the closest vector to \mathbf{t} in a single vector basis. This can be done exactly by finding the correct multiple of the only basis vector that is closest to \mathbf{t} .

When $n > 1$, we see that each run of the algorithm finds two candidates \mathbf{z}_1 and \mathbf{z}_2 . We show that the shorter of the two is an approximation to the closest vector to \mathbf{t} in $\mathbb{L}(\mathbf{B})$ for which

$$\|\mathbf{z} - \mathbf{t}\| \leq \sqrt{n}\gamma^2 \mathbf{d}(\mathbf{t}, \mathbf{B}) \quad (1)$$

We divide the proof in two cases, depending on whether $\mathbf{d}(\mathbf{t}, \mathbf{B}) < \frac{\lambda_1(\mathbf{B})}{2\gamma}$. It is sufficient to show that in each case one of \mathbf{z}_1 or \mathbf{z}_2 satisfies Equation (1).

1. If $\mathbf{d}(\mathbf{t}, \mathbf{B}) < \frac{\lambda_1(\mathbf{B})}{2\gamma}$, the promise of $\frac{1}{2\gamma}$ -BDD is satisfied. Thus, \mathbf{z}_1 satisfies $\|\mathbf{z}_1 - \mathbf{t}\| \leq \mathbf{d}(\mathbf{t}, \mathbf{B})$.
2. If $\mathbf{d}(\mathbf{t}, \mathbf{B}) \geq \frac{\lambda_1(\mathbf{B})}{2\gamma}$ we proceed as in Kannan's proof to show that \mathbf{z}_2 satisfies Equation (1).

By the induction hypothesis, \mathbf{z}'_2 satisfies

$$\|\mathbf{z}'_2 - \mathbf{t}'_{\perp \mathbf{v}}\|^2 \leq (n-1)\gamma^4 \mathbf{d}^2(\mathbf{t}'_{\perp \mathbf{v}}, \mathbf{B}'_{\perp \mathbf{v}})$$

At this point, note first that $\mathbf{t} = \mathbf{t}'_{\perp \mathbf{v}} + \phi \mathbf{v}$ for some $\phi \in \mathbb{R}$. Since also $\sum_{i=2}^n a_i \mathbf{b}_i = \mathbf{z}'_2 + \eta \mathbf{v}$ for some $\eta \in \mathbb{R}$, we can write

$$\begin{aligned} \|\mathbf{z}_2 - \mathbf{t}\|^2 &= \|(a_1 \mathbf{v} + \mathbf{z}'_2 + \eta \mathbf{v}) - (\mathbf{t}'_{\perp \mathbf{v}} + \phi \mathbf{v})\|^2 \\ &= \|(a_1 + \eta - \phi) \mathbf{v}\|^2 + \|\mathbf{z}'_2 - \mathbf{t}'_{\perp \mathbf{v}}\|^2 \end{aligned}$$

Since a_1 is chosen such that this expression is minimal we have $|a_1 + \eta - \phi| \leq \frac{1}{2}$, and so

$$\begin{aligned} \|\mathbf{z}_2 - \mathbf{t}\|^2 &\leq \|\mathbf{z}'_2 - \mathbf{t}'_{\perp \mathbf{v}}\|^2 + \frac{\|\mathbf{v}\|^2}{4} \leq \|\mathbf{z}'_2 - \mathbf{t}'_{\perp \mathbf{v}}\|^2 + \frac{\gamma^2 \lambda_1^2(\mathbf{B})}{4} \\ &\leq (n-1)\gamma^4 \mathbf{d}^2(\mathbf{t}'_{\perp \mathbf{v}}, \mathbb{L}(\mathbf{B}_{\perp \mathbf{v}})) + \frac{\gamma^2 4\gamma^2 \mathbf{d}^2(\mathbf{t}, \mathbf{B})}{4} \\ &\leq \gamma^4 n \mathbf{d}^2(\mathbf{t}, \mathbf{B}). \end{aligned}$$

The second last inequality follows from $\lambda_1^2(\mathbf{B}) \leq 4\gamma^2 \mathbf{d}^2(\mathbf{t}, \mathbf{B})$, which holds in this second case. To see the last inequality, note that $\mathbb{L}(\mathbf{B}_{\perp \mathbf{v}})$ is a projection of $\mathbb{L}(\mathbf{B})$ and $\mathbf{t}_{\perp \mathbf{v}}$ is a projection of \mathbf{t} in the direction orthogonal to \mathbf{v} , and a projection cannot increase the length of a vector.

Thus, in both cases one of \mathbf{z}_1 and \mathbf{z}_2 satisfies the requirements, and so we get the result. \square

5 Analysis of runtime

In this section, we show that Algorithm 1 runs in polynomial time. Observe first that in each recursive call the number of basis vector reduces by 1. Since all steps are obviously polynomial, it is enough to show that all the vectors generated during the run of the algorithm can be represented in polynomially

many bits in the input size of the top level of the algorithm. For this, we can assume that the original basis vectors $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ are integer vectors. This can be achieved by multiplying them with the product of their denominators. This operation does not increase the bit representation by more than a factor of $\log(mn)$. Assuming that the basis vectors are over integers, a lower bound on the input size can be given by $M = \max\{n, \log(\max_i \|\mathbf{b}_i\|)\}$.

Given a basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$, the Gram-Schmidt orthogonalization of \mathbf{B} is $\{\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_n\}$, where $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mathbf{b}_i|_{\tilde{\mathbf{b}}_j}$. We need the following Lemma from [9].

Lemma 3. [9] *Let $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ be n linearly independent vectors. Define the vectors $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mathbf{b}_i|_{\tilde{\mathbf{b}}_j}$. Then, the representation of any vector $\tilde{\mathbf{b}}_i$ as a vector of quotients of natural numbers takes at most $\text{poly}(M)$ bits for $M = \max\{n, \log(\max_i \|\mathbf{b}_i\|)\}$.*

Lemma 4. *Let \mathbf{v}_i , $i \in [n]$, be the vector \mathbf{v} generated in the i th level of the recursion in line 6 of Algorithm 1.*

There is a basis $\mathbf{x}_1, \dots, \mathbf{x}_n$ of \mathbf{B} such that the vectors \mathbf{v}_i are given by the Gram-Schmidt orthogonalization of $\mathbf{x}_1, \dots, \mathbf{x}_n$. Furthermore, $\mathbf{x}_1, \dots, \mathbf{x}_n$ as well as $\mathbf{v}_1, \dots, \mathbf{v}_n$ are polynomially representable in M .

Proof. We first find lattice vectors $\mathbf{x}_1, \dots, \mathbf{x}_n \in \mathbb{L}(\mathbf{B})$ which satisfy

$$\mathbf{x}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \delta_j \mathbf{v}_j$$

for some $\delta_j \in [-\frac{1}{2}, \frac{1}{2}]$, and then show that these vectors satisfy the claim of the lemma.

To see that such vectors exist, let \mathbf{B}_j be the basis in the j th level of the recursion of Algorithm 1. Then, we note that given a vector in $\mathbb{L}(\mathbf{B}_j)$ one can find a lattice vector in $\mathbb{L}(\mathbf{B}_{j-1})$ at distance at most $\frac{\|\mathbf{v}_{j-1}\|}{2}$ in the direction of \mathbf{v}_{j-1} or $-\mathbf{v}_{j-1}$. We let \mathbf{x}_i be the vector obtained by doing such a lifting step repeatedly until we have a lattice vector in $\mathbb{L}(\mathbf{B})$.

The vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are exactly the Gram-Schmidt orthogonalization of $\mathbf{x}_1, \dots, \mathbf{x}_n$, because

$$\mathbf{v}_i = \mathbf{x}_i - \mathbf{x}_i|_{\mathbf{v}_1} - \mathbf{x}_i|_{\mathbf{v}_2} - \dots - \mathbf{x}_i|_{\mathbf{v}_{i-1}},$$

and so the vectors \mathbf{x}_i must also form a basis of $\mathbb{L}(\mathbf{B})$.

Also, we have for all $i \in [n]$:

$$\begin{aligned} \|\mathbf{x}_i\|^2 &\leq \|\mathbf{v}_i\|^2 + \frac{\|\mathbf{v}_{i-1}\|^2}{4} + \dots + \frac{\|\mathbf{v}_1\|^2}{4} \\ &\leq \sum_{j=1}^i \|\mathbf{v}_j\|^2 \\ &\leq n\gamma^2 \lambda_n^2(\mathbf{B}) \end{aligned} \quad (\text{From Lemma 2})$$

As $\mathbf{x}_1, \dots, \mathbf{x}_n$ are vectors in the integer lattice \mathbf{B} ; $\mathbf{x}_1, \dots, \mathbf{x}_n$ are polynomially representable in M (and $\log \gamma$, but we can assume $\gamma < 2^n$). Coupled with Lemma 3 this completes the proof. \square

Lemma 5. *All vectors which are generated in a run of Algorithm 1 have a representation of size $\text{poly}(M)$ for $M = \max\{n, \log(\max_i \|b_i\|)\}$, in case the entries are represented as quotients of natural numbers.*

Proof. The vectors \mathbf{v}_i which are generated in line 6 at different levels of recursion also have representation of size $\text{poly}(M)$ by Lemma 3. The basis \mathbf{B}_i is LLL reduced and hence it is representable in number of bits which is a fixed polynomial in the shortest vector [14] and hence also \mathbf{v}_i .

The remaining vectors are produced by oracles which run in polynomial time or are small linear combinations of other vectors. \square

We now give a proof of Theorem 2.

Proof. (Theorem 2) Given $\mathbf{B} \in \mathbb{Q}^{m \times n}$ and $\mathbf{t} \in \mathbb{R}^m$ we run Algorithm 1. From Lemma 3, the algorithm returns a vector \mathbf{z} which is a $\gamma^2 \sqrt{n}$ -approximation to the closest vector. Also, from Lemma 5, all vectors in the algorithm have polynomial size representation, and so the algorithm runs in time $\text{poly}(\log \gamma, M)$. \square

6 Acknowledgements

We thank Divesh Aggarwal and Robin Künzler for numerous helpful discussions, and Daniele Micciancio for useful comments on an earlier version of this paper. We want to thank the anonymous referees for helpful comments. In particular, we thank the referee who pointed out the relevance of Theorem 1 to our work and helped us simplify the proof to its current form.

References

1. M. Ajtai. Generating hard instances of lattice problems, *STOC*, 1996, 99108.
2. M. Ajtai. The shortest vector problem in ℓ_2 is **NP**-hard for randomized reductions, *STOC*, 1998, 10-19.
3. Miklós Ajtai, Ravi Kumar and D. Sivakumar. Sampling Short Lattice Vectors and the Closest Lattice Vector Problem, *CCC*, 2002, pp. 53-57.
4. M. Ajtai, R. Kumar and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem, *STOC*, 1998, 266-275.
5. J. Blömer and J.-P. Seifert. The complexity of computing short linearly independent vectors and short bases in a lattice, *STOC*, 1999, 711-720.
6. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296:625-635, 1993.
7. I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is **NP**-hard. *Combinatorica*, 23(2):205243, 2003.
8. O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2):5561, 1999.

9. S. Goldwasser and D. Micciancio. Complexity of lattice problems, *Springer*, 2002.
10. I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors, *STOC*, 2007.
11. Ravi Kannan. Minkowski's convex body theorem and integer programming, *Math. Oper. Res.*, 12 (1987), pp. 415-440.
12. Ravi Kannan. Algorithmic geometry of numbers, *Annual Review of Computer Science* 2 (1987), 231-267.
13. S. Khot. Hardness of approximating the shortest vector problem in lattices, *JACM*, 2005, 52(5), 789-808.
14. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovasz. Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261(1982), 513-534.
15. Vadim Lyubashevsky, Daniele Micciancio. On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem, *CRYPTO 2009*, 577-594
16. D. Micciancio. Efficient reductions among lattice problems, *SODA*, 2008, 8493.
17. D. Micciancio. The shortest vector problem is **NP**-hard to approximate within some constant, *SIAM journal on Computing*, 2001, 30(6), 2008-2035.
18. D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations, *STOC*, 2010, pp. 351-358.
19. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem, *STOC*, 2009.
20. O. Regev. New lattice-based cryptographic constructions, *J. ACM* 51 (2004), no. 6, 899-942.
21. C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms, *Theoretical Computer Science*, 53(2-3):201-224, 1987.

A Solving BDD using a uSVP-oracle

In this appendix we sketch the reduction from $\text{BDD}_{1/2\gamma}$ to uSVP_γ from [15] for completeness. We will assume that $\mathbf{d}(\mathbf{t}, \mathbb{L}(\mathbf{B}))$ is known – it is shown in [15] how to avoid this assumption.

Proof. (Theorem 1) Let (\mathbf{B}, \mathbf{t}) be an instance of $\text{BDD}_{\frac{1}{2\gamma}}$ and let $\alpha = \mathbf{d}(\mathbf{t}, \mathbb{L}(\mathbf{B})) \leq \frac{\lambda_1(\mathbf{B})}{2\gamma}$. For simplicity we assume that we know α (see [15] for bypassing this). Our goal is to find a vector $\mathbf{t}^\dagger \in \mathbb{L}(\mathbf{B})$ such that $\mathbf{d}(\mathbf{t}^\dagger, \mathbf{t}) = \alpha$. We define the new basis

$$\tilde{\mathbf{B}} = \begin{pmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & \alpha \end{pmatrix}. \quad (2)$$

We will show that in $\tilde{\mathbf{B}}$ the vector $\mathbf{v} := \begin{bmatrix} \mathbf{t}^\dagger - \mathbf{t} \\ -\alpha \end{bmatrix}$ is a γ -unique shortest vector. It is clear that we can recover \mathbf{t}^\dagger , the solution to the BDD problem, when given \mathbf{v} . The length of \mathbf{v} is $\sqrt{2}\alpha$, and so it is enough to show that all other vectors in $\mathbb{L}(\tilde{\mathbf{B}})$, which are not a multiple of \mathbf{v} have length at least $\sqrt{2}\gamma\alpha$. Let us (for the sake of contradiction) assume that there is a vector \mathbf{v}_2 of length at most $\|\mathbf{v}_2\| < \sqrt{2}\gamma\alpha$ which is not a multiple of the vector \mathbf{v} above. We can write \mathbf{v}_2 as $\mathbf{v}_2 = \begin{bmatrix} \mathbf{u} - a\mathbf{t} \\ -a\alpha \end{bmatrix}$, where $\mathbf{u} \in \mathbb{L}(\mathbf{B})$ and $a \in \mathbb{Z}$. Since \mathbf{v}_2 is not a multiple of \mathbf{v} , it

must be that $\mathbf{u} - a\mathbf{t}^\dagger \in \mathbb{L}(\mathbf{B})$ is a non-zero lattice vector. Now, using the triangle inequality, we get

$$\begin{aligned}
\|\mathbf{u} - a\mathbf{t}^\dagger\| &\leq \|\mathbf{u} - a\mathbf{t}\| + a\|\mathbf{t} - \mathbf{t}^\dagger\| \\
&= \sqrt{\|\mathbf{v}_2\|^2 - a^2\alpha^2} + a\alpha \\
&< \sqrt{2\alpha^2\gamma^2 - a^2\alpha^2} + a\alpha \\
&\leq 2\alpha\gamma \leq \lambda_1(\mathbf{B}) , \qquad (\text{Maximized when } a = \gamma)
\end{aligned}$$

which is a contradiction. \square